Red Hat

Mark Nissley <mnissley@redhat.com>

[DCCSCR-Leadership] Anchore Container Findings

Hayden Smith <hsmith@anchore.com> Tue, Jan 21, 2020 at 1:40 PM
To: Mark Nissley <mnissley@redhat.com>, Taylor Biggs <taylor@redhat.com>
Cc: Jeremy Valance <jvalance@anchore.com>

Taylor/Mark—

I wanted to make sure we are tracking the issues in this thread Nic pointed out.

Most importantly is the Anchore upgrade that needs to occur as Nic suggests. I was midway through this process before I had to step out.
Can we make sure this is taken care of in the next two weeks and added to current tasking?
To help, I wanted to leave you in the good hands of Jeremy Valance (cc'd) who can assist Khary/Dino or whom ever picks up the ticket to upgrade Anchore. Jeremy is ready to help and can hop on blue jeans to assist if needed.

Please let me know so I can inform my leadership ASAP.

Vr
Hayden

---------- Forwarded message ---------
From: **Paul Holt** <paul@anchore.com>
Date: Mon, Jan 20, 2020 at 11:20 AM
Subject: Fwd: [Non-DoD Source] Anchore Container Findings
To: Kevin O'Donnell <kodonnel@redhat.com>, Taylor Biggs <tbiggs@redhat.com>
CC: Daniel Nurmi <nurmi@anchore.com>, Neil Levine <nlevine@anchore.com>, Jeremy Valance <jvalance@anchore.com>

Hi Kevin and Taylor,

We'd like to get a call arranged in the next day or so to discuss how we can support the Red Hat team in addressing the relevant issues that are raised in the exchanges below. It is a top priority for us to get sorted and we think we have some good suggestions on how we can make positive progress.

Let me know your thoughts and time slots that might work?

Thanks
Paul

---------- Forwarded message ---------
From: **Daniel Nurmi** <nurmi@anchore.com>
Date: Sun, Jan 19, 2020 at 12:48 PM
Subject: Re: [Non-DoD Source] Anchore Container Findings
To: Chaillan, Nicolas M HQE USAF SAF-AQ (USA) <nicolas.m.chaillan.civ@mail.mil>
Cc: mhuston.wir@diu.mil <mhuston.wir@diu.mil>, The purpose of this list is to consolidate the e-mail addresses necessary for contacting the leadership of the DCCSCR team. <dccscr-leadership@redhat.com>, Hayden Smith <hsmith@anchore.com>, paul@anchore.com <paul@anchore.com>, Said Ziouani <saidz@anchore.com>, Taylor Biggs <taylor@redhat.com>

Nic,

Some further information inline, below:

On Sun, Jan 19, 2020 at 7:10 AM Chaillan, Nicolas M HQE USAF SAF-AQ (USA) <nicolas.m.chaillan.civ@mail.mil> wrote:

> Thanks Daniel,
>
> See my answers below, thanks for the quick reply.
>
> Taylor, Matt, please work with Daniel below to COMPLETELY automate the Anchore updates of containers and feeds. This should be the case for ALL containers.
>
> Best regards,
>
> Nicolas M. Chaillan, HQE
>
> Chief Software Officer, Air Force
>
> Co-Lead DoD Enterprise DevSecOps Initiative
>
> Pentagon 5E741
>
> Office: (703) 693 4740
>
> Cell: 202-421-9845
>
> Office of the Chief Software Officer: https://software.af.mil - usaf.cso@mail.mil
>
> **From:** Daniel Nurmi <nurmi@anchore.com>
> **Sent:** Sunday, January 19, 2020 12:20 AM
> **To:** Chaillan, Nicolas M HQE USAF SAF-AQ (USA) <nicolas.m.chaillan.civ@mail.mil>
> **Cc:** mhuston.wir@diu.mil; The purpose of this list is to consolidate the e-mail addresses necessary for contacting the leadership of the DCCSCR team. <dccscr-leadership@redhat.com>; Hayden Smith <hsmith@anchore.com>; paul@anchore.com; Said Ziouani <saidz@anchore.com>
> **Subject:** Re: [Non-DoD Source] Anchore Container Findings
>
> All active links contained in this email were disabled. Please verify the identity of the sender, and confirm the authenticity of all links contained within the message prior to copying and pasting the address to a Web browser.
>
> ---
>
> Nic,
>
> Thank you for the detailed response - I can share some of the context and latest status of several of the observed concerns, here. One important point is that, while we wanted to quickly annotate and get back the four result sheets for

> your review as soon as possible, that while they really are an accurate reflection of the last stable images that are in the DCAR, I wanted to make it clear, here, that we've already taken steps to remediate the findings, which will then manifest in the very next anchore release scheduled shortly.
>
> Overall, the critical point is: with an Anchore team member embedded into the DCCSCR team, you very well know that my mandate from day 1 is to have COMPLEME automation to get container updates and data feeds. I'm shocked to learn we don't have that for our critical product like Anchore. We need the process to be SEAMLESS and COMPLETELY automated with no human in the loop when you release an update. This is a top priority and must be done within 15 days. Taylor/Matt let's make this happen.
>
> 1) (RH feeds finding) : In december, the RH security data (from upstream RH) experienced an alteration that broke compatibility with the anchore feed driver - we were able to quickly introduce code to fix which made its way into the december anchore enterprise 2.2 release. Shortly after, we conveyed the information that an upgrade would be required to remedy the feed issue - the current status of the upgrade from the last update I received on wed. was that the upgrade was in progress - we'll double check again on the status of the software upgrade. While the holidays likely contributed to some delay, we do feel that this process can be made more efficient, so that upgrades in the future be implemented in a more timely manner.
>
> Again, this needs to be raised in criticality and should have been already automated. There should be NO HUMAN INVOLVEMENT in this process

We're available to work with the team that deploys and manages the anchore deployment on this - I don't want to speak out of turn on status, but I can report on the fact that in Dec, we received some updated requirements on the container image builds (setting the standard for all vendors) which was very much in line with some of the original plans that we had prepared for. We immediately were able to update our build processes to satisfy all of the requirements for automated image builds and implemented them prior to the holidays - currently, the anchore build process in the project should ensure that as soon as anchore releases a new patch/software update, the new images themselves should be built according to the stated requirements in the DCAR.

> 2) (Dependency updates) : When we ran our latest scans against anchore engine/enterprise containers in Dec, we took the action (this was before the scanning results, I wanted to assure yo uthat we are proactively monitoring and updating dependencies as best as we can) to begin testing the system against the latest python dependencies, which took some work as some of the dependency updates lead to breaking functionality, which ultimately didn't make the last stable release. Currently, the regular python dependencies (several of those noted in the report, but also most others as well) have already been updated to the very latest (and tested), which will be availlable in the very next release of anchore engine, scheduled to be available by the end of January. In addition, our engineering team has also updated the nodeJS dependencies included in the enterprise UI as well.
>
> Perfect
>
> 3) (Swagger UI) : Anchore engine uses the flask/connextion framework, even the latest of which includes those embedded swagger-ui 'min.js' code snippets that were discovered in the scans. Since those don't come in a regular way (i.e. they are not versions that we can update, since the 'flask/connextion' packages include those older versions), we took the action to mitigate the potential exposure by introducing an option to disable the flask swagger-ui capability entirely. We can explore with you the option of manually removing these code bits from the official flask/connextion packages if that is a solution that you would prefer, though we would recommend disabling the swagger-ui entirely given that the upstream latest is using outdated, embedded code.

> I would actually recommend REMOVING the code. Disabling isn't good enough. Bad actor would still find a way to use it as lateral movement… Also, I would recommend changing your dependencies when you feel what you're using is putting you in such a predicament! There is no such excuse of "this isn't me, it is my dependency.".

These particular pieces of code are client side UI elements that are enabled only when the developer/debug 'swagger-ui' functions of the flask/connexion framework are enabled (which they are by default). Since they are not part of anchore itself (i.e. this isn't code that is loaded in anchore, nor is anchore code accessible via a browser/UI in this context), and also not loaded when the feature of the flask framework is disabled (there is no nodeJS runtime in these images, thus also there is not a way to execute the code, server-side), we feel that the disable capability is the most important step to take to reduce this (and future) problems in this area. Generally the swagger-ui is only something that users would only temporarily enable as a convenience when investigating clients/integrations with anchore, but again isn't part of the functionality of the system. Disabling the route makes those nodeJS snippets that are client-side, for UI display/formatting in the swagger-ui, unloaded and inaccessible.

We can discuss manual removal of these snippets with the build team if you feel that our solution is insufficient, though generally we (all) need to be mindful of the implications of triggering OSS license conditions as a result of modifying OSS software (not our own, but in cases like this dependencies that are several levels removed from the top level). Instead, we're planning to at the very least prod the upstream to see if we can work with them to (minimally) update the versions of the dependencies that they're embedding and/or (ideally) altering their own build mechanisms to be more dynamic / standard when it comes to pulling in deps, rather than having the code hard embedded and version locked.

> 4) (Report Content/Clarity) : We agree that these generated reports/format are somewhat confusing - anchore itself produces a lot more information about the various findings than is being displayed in the spreadsheet, and we had a discussion this last thursday internally about this specific topic. We intend to initiate a discussion with the team operating anchore/producing the reports about how to extract additional information and context that would make the report clearer and more actionable by the vendors. As these are some of the first real round of results that we've had the ability to review, we've additionally discussed improvements to the next round of policy updates to better sanitize the duplicated results (inherited from base) which we believe will also help to improve the quality of the information in the spreadsheets.
>
> OK, let's work with DCCSCR to get these piloted ASAP

Agreed! We'll be following up on these topics, with the team.

Thank you Nic!

Best Regards,
-Daniel Nurmi
CTO, Co-founder - Anchore

> In sum - we've taken a number of steps to remedy the findings, improve our process of dependency review to be early in a major development cycle in order to head off breaking major functionality issues, are working with the anchore deployment team on upgrading to the Dec release of anchore enterprise (including the update that resolve the RH feeds finding), and have ideas and plans for improving the report quality - we're actively working on these topics!
>
> Please reach out If you would like to discuss any of these items further, or let us know if you would like us to adjust any of the above plans!
>
> Best Regards,

> -Daniel Nurmi
>
> CTO, Co-founder - Anchore
>
> On Sat, Jan 18, 2020 at 7:21 PM Chaillan, Nicolas M HQE USAF SAF-AQ (USA) <nicolas.m.chaillan.civ@mail.mil < Caution-mailto:nicolas.m.chaillan.civ@mail.mil > > wrote:
>
>> Daniel,
>>
>> Please find the first 2 containers and their status.
>>
>> You will see a new column called NC where you will find risk accepted/rejected or accepted with conditions. If those conditions aren't met in due time, the container will be removed from DCAR.
>>
>> Additionally, it seems you have not automated the download of Anchore feeds in DCCSCR/DCAR. This was mandated day 1… I don't understand how your team didn't do that as you have someone embedded in the team. This really makes no sense. That's like step 0. This has to be addressed as a TOP PRIORITY within 30 days. Everything, including all your containers must automatically update at the SAME TIME you have a release.
>>
>> I had to reject some of your containers due to dependencies like Swagger UI from 2016… This is really unacceptable from a security company standpoint. You need to step up your game here! How did you miss this and why isn't your own scanner detecting this when Twistlock does?!
>>
>> Finally, I really feel we get better and more information on the Twistlock report. If you compare with the Anchore results, we don't get as much results; I really don't understand why the CVE isn't in a separate column just with the CVE etc. Doesn't provide score etc. How can we fix this and make it look like the Twistlock report?! Also your link in your description "check_output" column, points to a local API from Anchore, this is useless. Why can't you have this hosted on your domain so people can review it from anywhere? I don't have access to the local Anchore URL as I'm not on Kubernetes on the cluster…
>>
>> I expect security companies to PROACTIVELY fix findings and dependencies. It seems you have things from April 2019…
>>
>> Thank you!
>>
>> Best regards,
>>
>> Nicolas M. Chaillan, HQE
>>
>> Chief Software Officer, Air Force

> > Co-Lead DoD Enterprise DevSecOps Initiative
> >
> > Pentagon 5E741
> >
> > Office: (703) 693 4740
> >
> > Cell: 202-421-9845
> >
> > Office of the Chief Software Officer: Caution-https://software.af.mil < Caution-https://software.af.mil > - usaf.cso@mail.mil < Caution-mailto:usaf.cso@mail.mil >
> >
> > **From:** Daniel Nurmi <nurmi@anchore.com < Caution-mailto:nurmi@anchore.com > >
> > **Sent:** Wednesday, January 15, 2020 1:35 PM
> > **To:** Chaillan, Nicolas M HQE USAF SAF-AQ (USA) <nicolas.m.chaillan.civ@mail.mil < Caution-mailto:nicolas.m.chaillan.civ@mail.mil > >
> > **Cc:** mhuston.wir@diu.mil < Caution-mailto:mhuston.wir@diu.mil > ; The purpose of this list is to consolidate the e-mail addresses necessary for contacting the leadership of the DCCSCR team. <dccscr-leadership@redhat.com < Caution-mailto:dccscr-leadership@redhat.com > >; Hayden Smith <hsmith@anchore.com < Caution-mailto:hsmith@anchore.com > >
> > **Subject:** [Non-DoD Source] Anchore Container Findings
> >
> > Mr. Chaillan,
> >
> > Please see the attached sheets (4 total, one for each anchor enterprise container image). We're ready to discuss/clarify further the details for each finding, in the 'explanation' column for each sheet, at your convenience.
> >
> > Best Regards,
> >
> > Daniel Nurmi (Anchore)

--
Paul Holt
SVP Sales and Field Operations
703 424 5907

--
V/r
Hayden Smith
Senior Engineer
Anchore
Los Angeles, CA
Cell: (562) 676-5815